

Configuración de PBR con IP SLA para ISP DUAL en FTD administrado por FMC

Contenido

[Introducción](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Paso 1. Configurar lista de acceso PBR](#)

[Paso 2. Configurar mapa de ruta PBR](#)

[Paso 3. Configurar objetos de texto de FlexConfig](#)

[Paso 4. Configurar el monitor SLA](#)

[Paso 4. Configuración de Rutas Estáticas con Route Track](#)

[Paso 5. Configurar objeto FlexConfig de PBR](#)

[Paso 6. Asignación de un objeto FlexConfig PBR a una política FlexConfig](#)

[Verificación](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar PBR junto con IP SLAs en un FTD que es administrado por (FMC).

Colaboración de Daniel Perez Verti Vazquez, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración PBR activada **Cisco Adaptive Security Appliance (ASA)**
- FlexConfig en **Firepower**
- IP SLAs

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco FTD versión 7.0.0 (Compilación 94)

- Cisco FMC versión 7.0.0 (Compilación 94)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe cómo configurar **Policy Based Routing (PBR)** junto con **Internet Protocol Service Level Agreement (IP SLA)** en un dispositivo **CISCO Firepower Threat Defense (FTD)** que gestiona Cisco **Firepower Management Center (FMC)**.

El ruteo tradicional toma decisiones de reenvío basadas solamente en las direcciones IP de destino. PBR es una alternativa a los protocolos de ruteo y al ruteo estático.

Proporciona un control más granular sobre el ruteo porque permite el uso de parámetros como direcciones IP de origen o puertos de origen y destino como criterios de ruteo además de la dirección IP de destino.

Los escenarios posibles para PBR incluyen aplicaciones sensibles al origen o tráfico a través de links dedicados.

Junto con PBR, se pueden implementar IP SLAs para garantizar la disponibilidad del salto siguiente. Un SLA de IP es un mecanismo que monitorea la conectividad de extremo a extremo a través del intercambio de paquetes regulares.

En el momento de la publicación, PBR no se admite directamente a través de FMC **Graphical User Interface (GUI)**, la configuración de la función requiere el uso de políticas FlexConfig.

Por otro lado, solo **Internet Control Message Protocol (ICMP)** FTD admite los SLA.

En este ejemplo, PBR se utiliza para rutear paquetes a través de un primario **Internet Service Provider (ISP)** circuito basado en la dirección IP de origen.

Mientras tanto, un SLA de IP supervisa la conectividad y fuerza una reserva al circuito de respaldo en caso de que se produzca algún fallo.

Configurar

Diagrama de la red

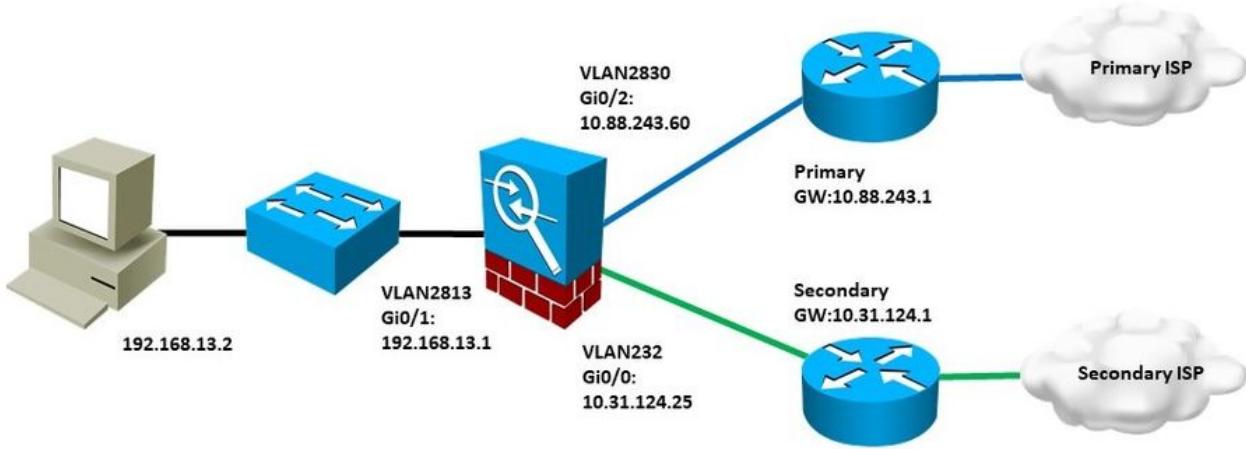
En este ejemplo, Cisco FTD tiene dos interfaces externas: VLAN230 y VLAN232. Cada uno se conecta a un ISP diferente.

El tráfico de la red interna VLAN2813 se enruta a través del ISP primario que utiliza PBR.

El mapa de ruta PBR toma decisiones de reenvío basadas solamente en la dirección IP de origen (todo lo recibido de VLAN2813 debe enrutarse a 10.88.243.1 en VLAN230) y se aplica en la interfaz GigabitEthernet 0/1 de FTD.

Mientras tanto, FTD utiliza IP SLAs para monitorear la conectividad a cada gateway ISP. En caso

de cualquier falla en VLAN230, las fallas FTD al circuito de respaldo en VLAN232.



Configuraciones

Paso 1. Configurar lista de acceso PBR

En el primer paso de la configuración PBR, defina qué paquetes deben estar sujetos a la política de ruteo. PBR hace uso de mapas de ruta y lista de acceso para identificar el tráfico.

Para definir una lista de acceso para los criterios coincidentes, navegue hasta **Objects > Object Management** y seleccione **Extended** en el **Access List** de la tabla de contenido.

The screenshot shows a network management interface with the following details:

- Header:** Overview, Analysis, Policies, Devices, **Objects** (highlighted), AMP, Intelligence.
- Sub-header:** Object Management, Intrusion Rules.
- Content Area:**
 - Left Sidebar (Table of Contents):** Extended, AAA Server, RADIUS Server Group, Single Sign-on Server, Access List (selected), Extended, Standard, Address Pools, IPv4 Pools, IPv6 Pools, Application Filters, AS Path, Cipher Suite List, Community List, Distinguished Name, Individual Objects, Object Groups, DNS Server Group, External Attributes, Dynamic Object, Security Group Tag, File List, FlexConfig.
 - Right Main Area:** A table titled "No records to display". It has columns: Name, Value, and Override.
- Bottom Status Bar:** Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2.
- Bottom Footer:** Action bar with icons for Add Extended Access List, Filter, and Cisco logo.

Haga clic en **Add Extended Access List**. En el **New Extended Access List Object**, asigne un nombre al objeto y seleccione la **Add** para comenzar con la configuración de la lista de acceso.

The screenshot shows the 'Objects' tab selected in the navigation bar. Under 'Object Management', the 'Extended' category is chosen. A new object is being created with the name 'PBR_ACL'. The 'Add' button in the top right corner of the entry table is highlighted with a red box.

En el **Add Extended Access List Entry** seleccione el objeto que representa la red interna, en este caso **VLAN2813**.

Haga clic en **Add to Source** para definirla como el origen de la lista de acceso.

Haga clic en **Add** para crear la entrada.

The screenshot shows the 'Add Extended Access List Entry' dialog. In the 'Network' tab, 'VLAN2813' is selected from the 'Available Networks' list and added to the 'Source Networks' list. The 'Add to Source' button is highlighted with a red box. The 'Add' button at the bottom right is also highlighted with a red box.

Haga clic en **Save**. El objeto debe agregarse a la lista de objetos.

The screenshot shows the ASA Object Management interface under the Objects tab. The left sidebar lists various object types like AAA Server, Access List, Address Pools, and External Attributes. The main pane displays an Extended Access List named "PBR_ACL". The table has columns for Name, Value, and Override. A red box highlights the "Name" column for "PBR_ACL".

Name	Value	Override
PBR_ACL		

Displaying 1 of 1 rows | < Page 1 of 1 > | C
Go to System in Control Panel to activate Windows.

Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

Paso 2. Configurar mapa de ruta PBR

Una vez configurada la lista de acceso PBR, asínghela a un route map. El mapa de ruta evalúa el tráfico en función de las cláusulas de coincidencia definidas en la lista de acceso.

Una vez que se produce una coincidencia, el route map ejecuta las acciones definidas en la política de ruteo.

Para definir el mapa de ruta, vaya a **Objects > Object Management** y seleccione **Route Map** en la tabla de contenido.

The screenshot shows the ASA Object Management interface under the Objects tab. The left sidebar lists various objects like Geolocation, Interface, Key Chain, Network, PKI, Policy List, Port, Prefix List, and Route Map. The "Route Map" item is highlighted with a red box. The main pane displays a table titled "Route Map" with columns for Name, Value, and Override. A message "No records to display" is shown. A red box highlights the "Name" column.

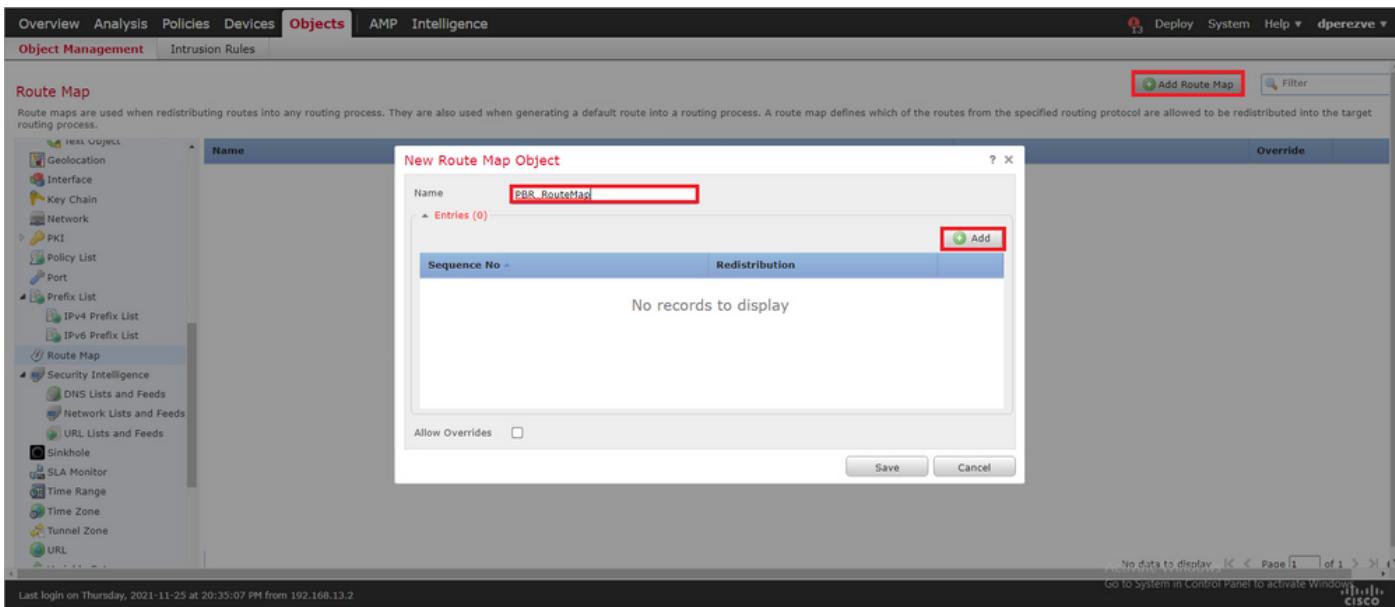
Name	Value	Override

No records to display

No data to display | < Page 1 of 1 > | C
Go to System in Control Panel to activate Windows.

Last login on Thursday, 2021-11-25 at 20:35:07 PM from 192.168.13.2

Haga clic en **Add Route Map >**. En el **New Route Map Object** asigne un nombre al objeto y haga clic en **Add** para crear una nueva entrada de mapa de ruta.



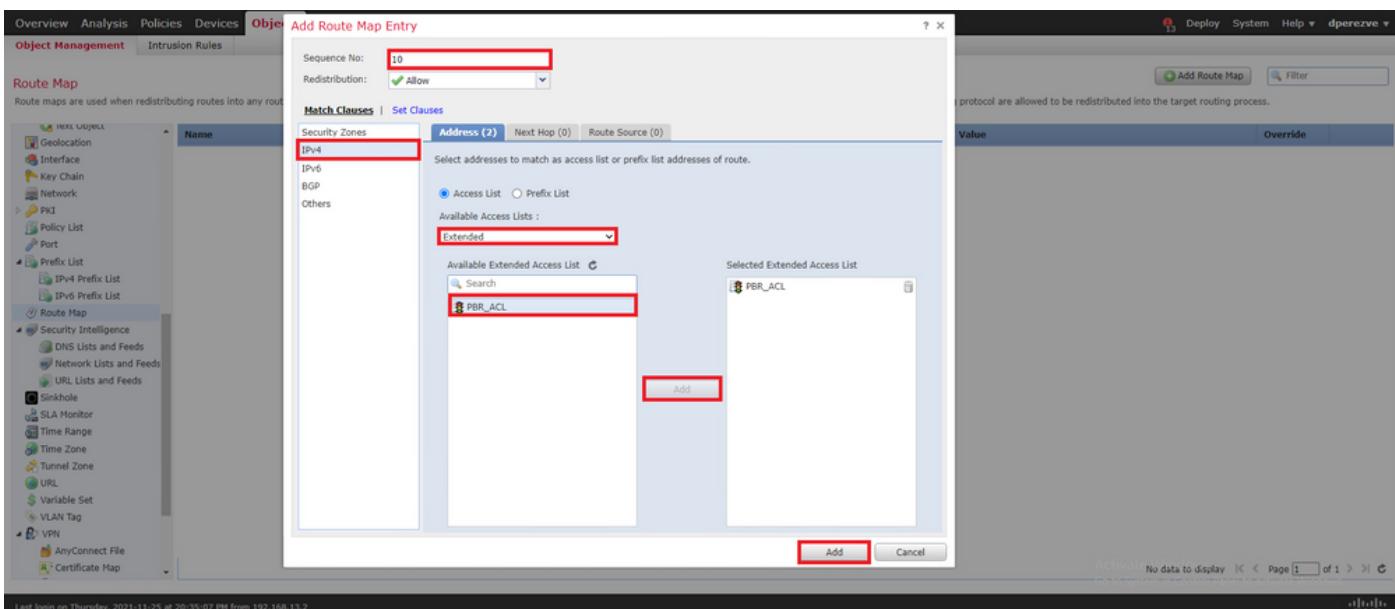
En el **Add Route Map Entry**, defina un número de secuencia para la posición de la nueva entrada.

Desplácese hasta **IPv4 > Match Clauses** y seleccione **Extendido** en el **Available Access List** menú desplegable.

Seleccione el objeto de lista de acceso creado en el paso 1.

Haga clic en **Add** para crear la entrada.

Nota: FTD admite hasta 65536 (de 0 a 65535) entradas diferentes. Cuanto menor sea el número, mayor será la prioridad de evaluación.



Haga clic en **Save**. Agregue el objeto a la lista de objetos.

Name	Value	Override
PBR_RouteMap		

Paso 3. Configurar objetos de texto de FlexConfig

El siguiente paso implica la definición de objetos de texto FlexConfig que representan puertas de enlace predeterminadas para cada circuito. Estos objetos de texto se utilizan más adelante en la configuración del objeto FlexConfig que asocia PBR con los SLA.

Para definir un objeto de texto FlexConfig, vaya a **Objects > Object Management** y seleccione **Text Object** en el **FlexConfig** de la tabla de contenido.

Name	Value	Type	Override
defaultDNSNameServerList	1.1.1.1	System Defined	
defaultDNSParameters	3 5 10 15 abc.com	System Defined	
disableInspectProtocolList		System Defined	
dnsNameServerList	2.2.2.2	System Defined	
dnsParameters	3 5 abc.com	System Defined	
eigrpAS	1	System Defined	
eigrpAuthKey		System Defined	
eigrpAuthKeyId		System Defined	
eigrpDisableAutoSummary	false	System Defined	
eigrpDisableSplitHorizon	false	System Defined	
eigrpHelloInterval	60	System Defined	
eigrpHoldTime	180	System Defined	

Haga clic en **Add Text Object**. En el **Add Text Object**, asigne un nombre al objeto que representa la puerta de enlace principal y especifique la dirección IPv4 para este dispositivo.

Haga clic en **Save** para agregar el nuevo objeto.

The screenshot shows the Cisco ASA configuration interface under the 'Objects' tab. In the left sidebar, 'Text Object' is selected. A modal window titled 'Add Text Object' is open, prompting for a name ('Primary_GW') and description. The variable type is set to 'Single' with a count of 1. The value field contains '10.88.243.1'. The 'Save' button at the bottom of the modal is highlighted with a red box.

Haga clic en **Add Text Object** de nuevo para crear un segundo objeto, esta vez para la puerta de enlace en el circuito de copia de seguridad.

Rellene el nuevo objeto con el nombre y la dirección IP adecuados y haga clic en **Save**.

This screenshot is identical to the previous one, showing the 'Add Text Object' dialog box. The new object is named 'Secondary_GW' and has the value '10.31.124.1'. The 'Save' button is again highlighted with a red box.

Los dos objetos deben agregarse a la lista junto con los objetos predeterminados.

Text objects define free-form text strings that you use as variables in a FlexConfig object. These objects can have single values or be a list of multiple values.

Name	Value	Type	Override
Primary_GW	10.88.243.1	User Defined	X
Secondary_GW	10.31.124.1	User Defined	X

Paso 4. Configurar el monitor SLA

Para definir los objetos SLA utilizados para supervisar la conectividad con cada gateway, vaya a Objects > Object Management y seleccione SLA Monitor en la tabla de contenido.

SLA monitor defines a connectivity policy to a monitored address and tracks the availability of a route to the address. The SLA Monitor object is used in the Route Tracking field of an IPv4 Static Route Policy. IPv6 routes do not have the option to use SLA monitor via route tracking.

Name	Value
No records to display	

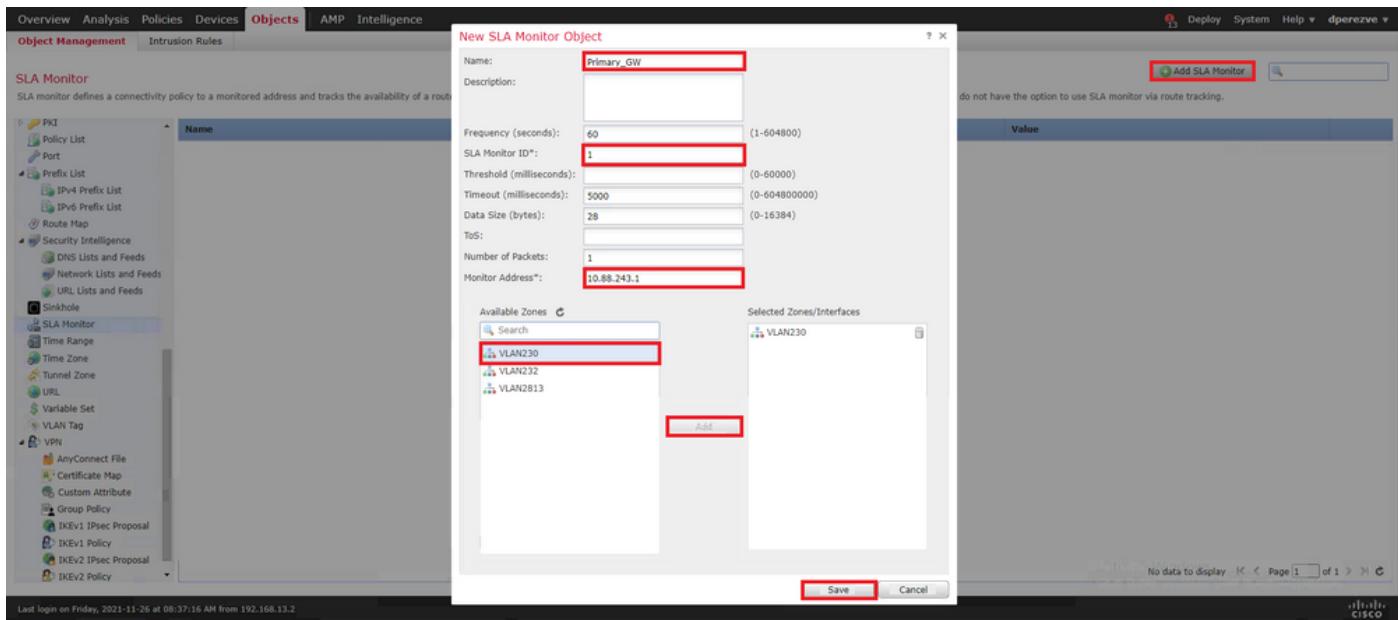
Seleccione el Add SLA Monitor objeto.

En el **New SLA Monitor**, defina un nombre junto con un identificador para la operación SLA, la dirección IP para el dispositivo que se debe monitorear (en este caso, el gateway principal) y la interfaz o zona a través de la cual se puede alcanzar el dispositivo.

Además, también es posible ajustar el tiempo de espera y el umbral. Haga clic en **Save**.

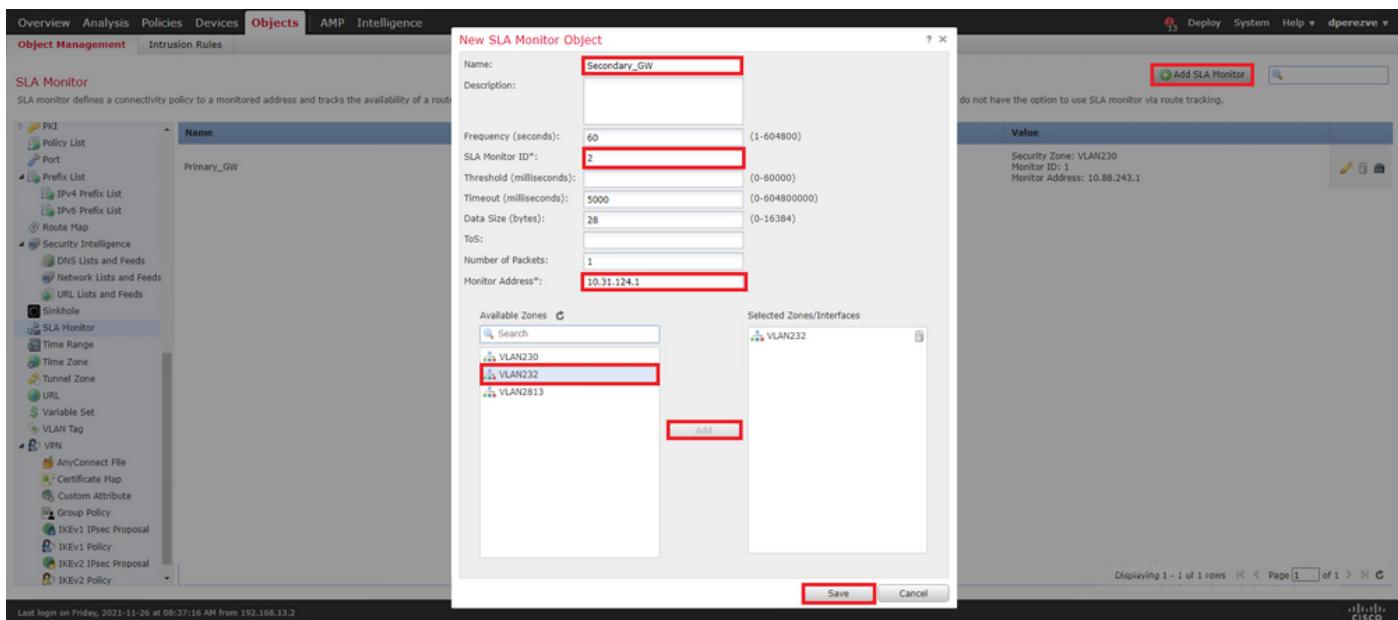
Nota: FTD admite hasta 2000 operaciones de SLA. Los valores para el ID de SLA van de 1 a 2147483647.

Nota: Si no se especifican valores de límite de tiempo y umbral, FTD utiliza temporizadores predeterminados: 5000 milisegundos en cada caso.



Seleccione el **Add SLA Monitor** una vez más para crear un segundo objeto, esta vez para la puerta de enlace en el circuito de copia de seguridad.

Rellene el nuevo objeto con la información adecuada, asegúrese de que el ID de SLA sea diferente del definido para el gateway principal y guarde los cambios.



Los dos objetos deben agregarse a la lista.

Name	Value
Primary_GW	Security Zone: VLAN230 Monitor ID: 1 Monitor Address: 10.88.243.1
Secondary_GW	Security Zone: VLAN232 Monitor ID: 2 Monitor Address: 10.31.124.1

Paso 4. Configuración de Rutas Estáticas con Route Track

Una vez creados los objetos de SLA de IP, defina una ruta para cada gateway y asóciela a los SLA.

En realidad, estas rutas no proporcionan conectividad desde el interior al exterior (todo el routing se realiza a través de PBR); en su lugar, son necesarias para realizar un seguimiento de la conectividad con las puertas de enlace a través de los SLA.

Para configurar rutas estáticas, navegue hasta **Devices > Device Management**, edite el FTD disponible y seleccione **Static Route** en la tabla de contenido dentro de la **Routing** ficha.

Network	Interface	Leaked from Virtual Router	Gateway	Tunneled	Metric	Tracked
▼ IPv4 Routes						
▼ IPv6 Routes						

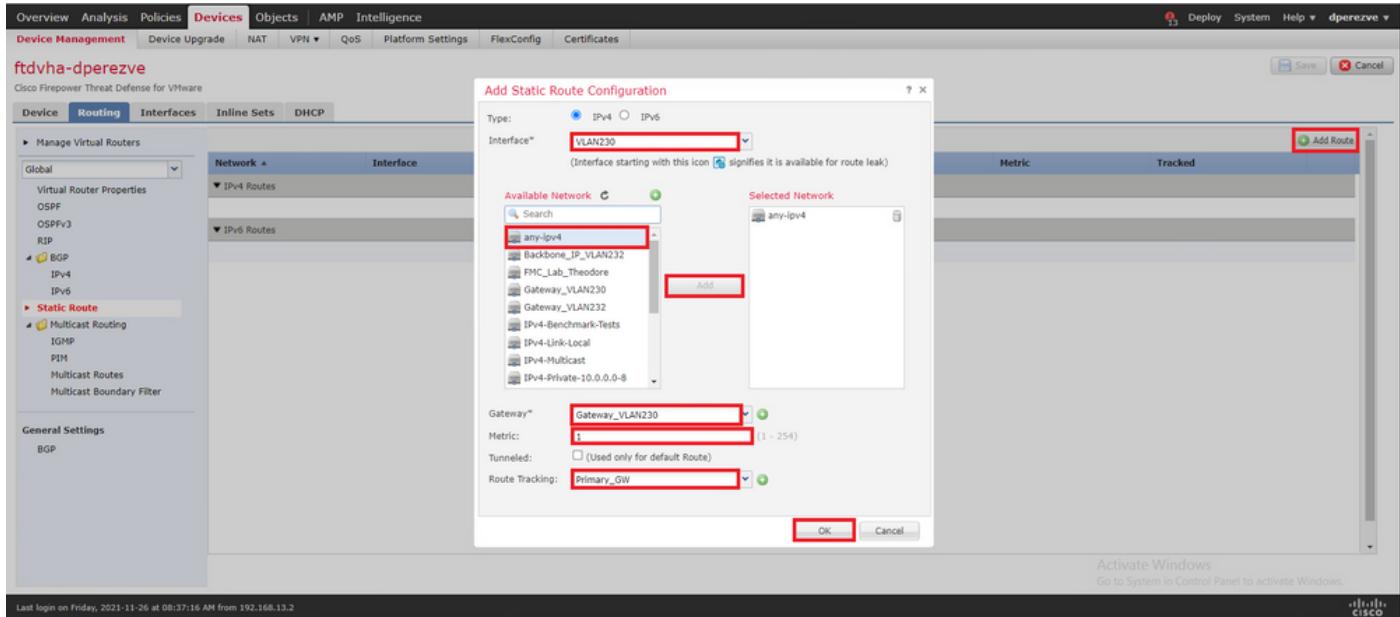
En el **Add Static Route Configuration**, en el menú desplegable **Interface**, especifique el nombre de la interfaz a través de la cual debe ser accesible la puerta de enlace principal.

A continuación, seleccione la red de destino y la puerta de enlace principal en el **Gateway** desplegable.

Especifique una métrica para la ruta y en el **Route Track** y seleccione el objeto SLA para el gateway

principal creado en el paso 3.

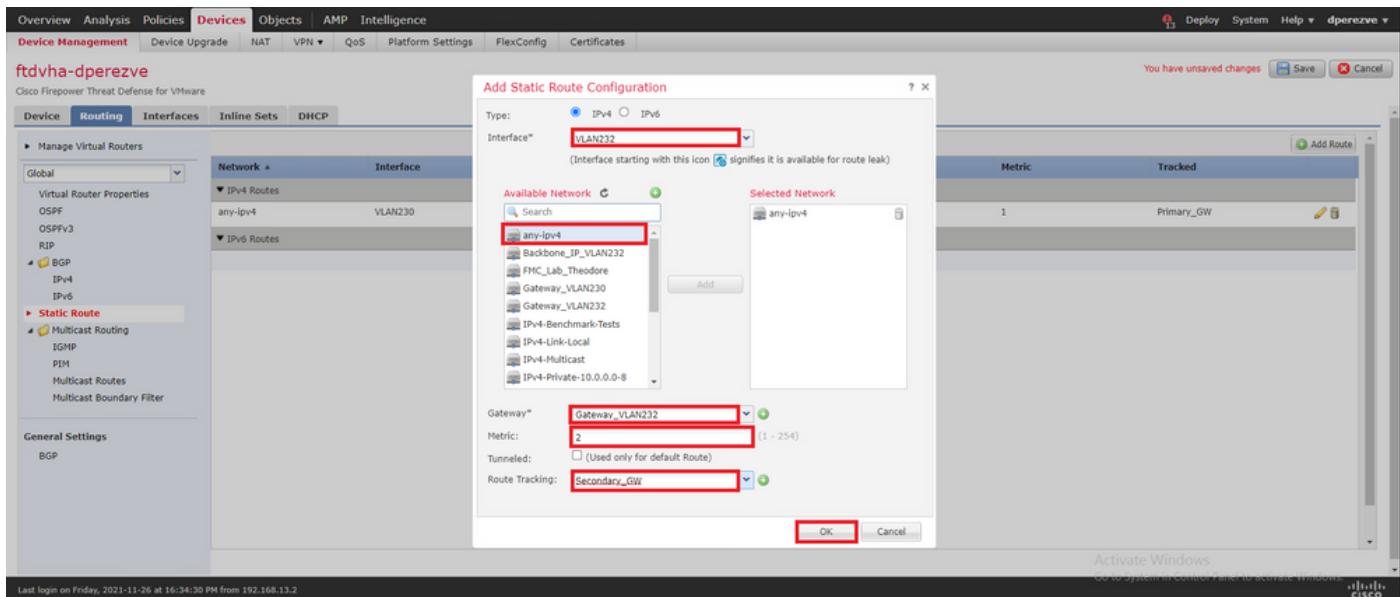
Haga clic en **Aceptar** para agregar la nueva ruta.



Se debe configurar una segunda ruta estática para la puerta de enlace de copia de seguridad.

Haga clic en **Add Route** para definir una nueva ruta estática.

Rellene el **Add Static Route Configuration** con la información para la gateway de respaldo y asegúrese de que la métrica para esta ruta sea mayor que la configurada en la primera ruta.



Las dos rutas deben agregarse a la lista.

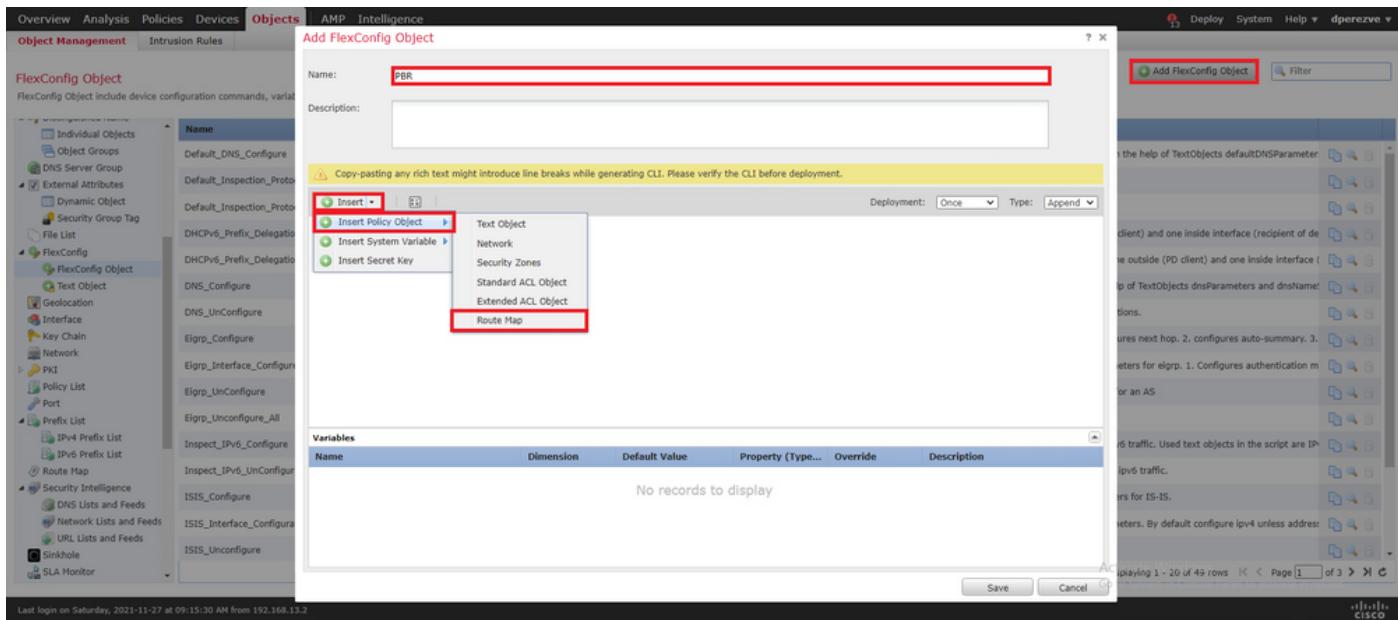
Paso 5. Configurar objeto FlexConfig de PBR

Habilite los SLA en el route map utilizado para PBR y aplique este route map en una interfaz del FTD.

Hasta ahora, el mapa de ruta sólo se ha asociado a la lista de acceso que define los criterios coincidentes. Sin embargo, los últimos ajustes no se admiten a través de la GUI de FMC, por lo que se necesita un objeto FlexConfig.

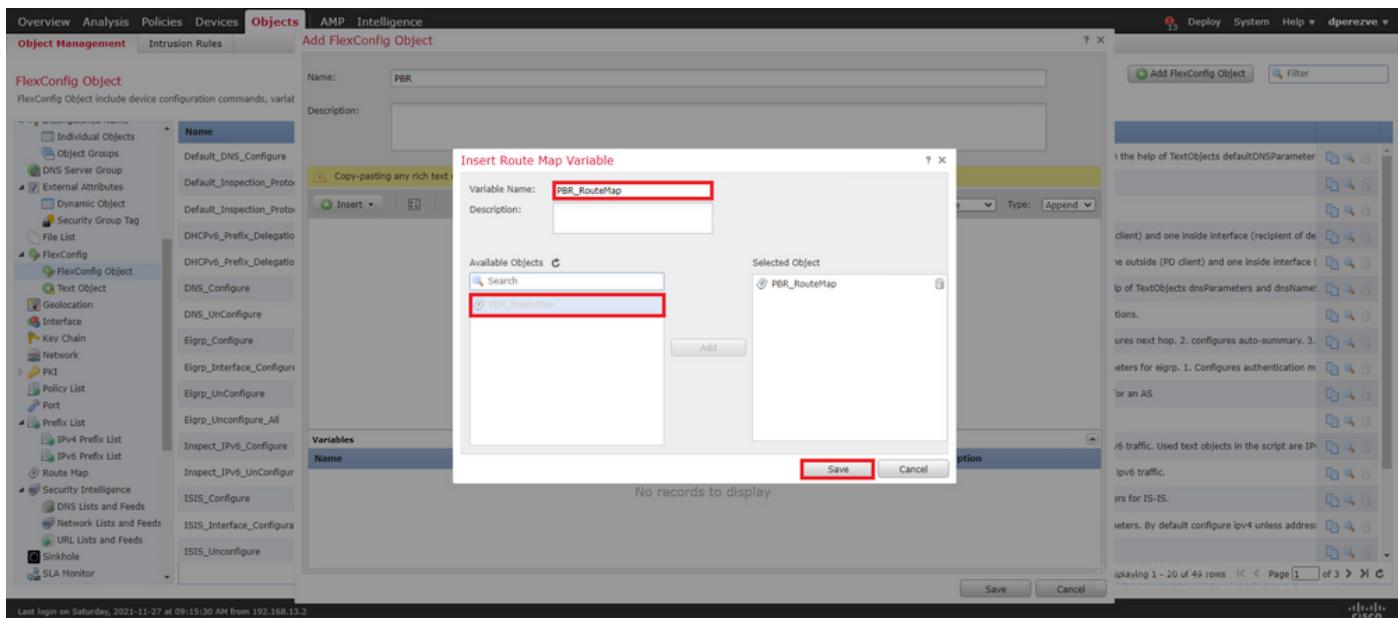
Para definir el objeto FlexConfig de PBR, vaya a Objects > Object Management y seleccione FlexConfig Object en el FlexConfig de la tabla de contenido.

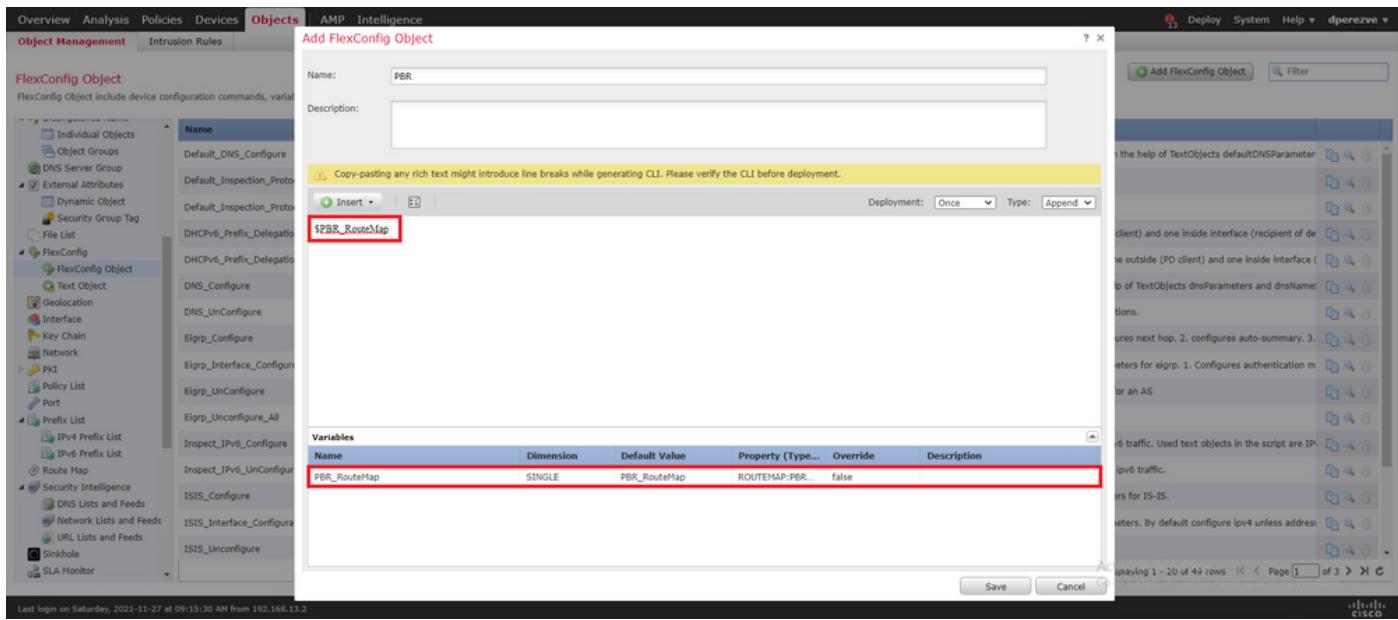
Seleccione el Add FlexConfig Object botón. En el Add FlexConfig Object asignar un nombre y desplazarse hasta Insert > Insert Policy Object > Route Map .



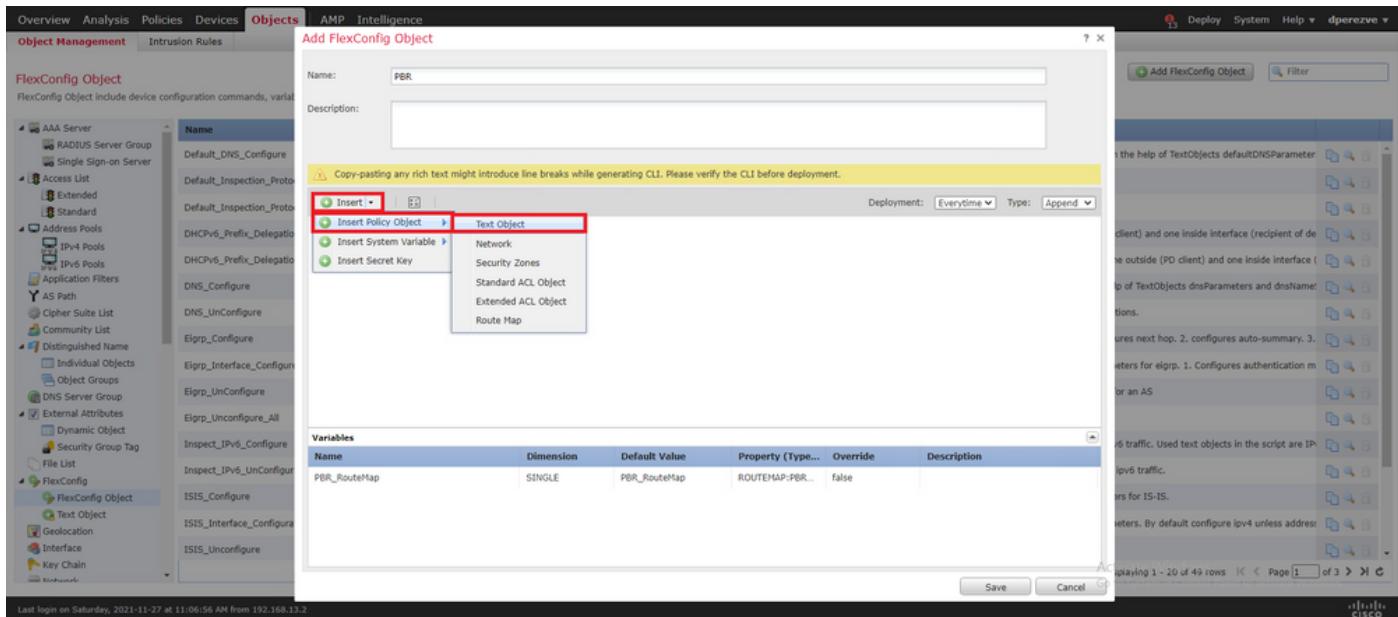
En el **Insert Route Map Variable**, asigne un nombre a la variable y seleccione el objeto PBR creado en el paso 2.

Haga clic en **Save** para agregar el mapa de ruta como parte del objeto FlexConfig.



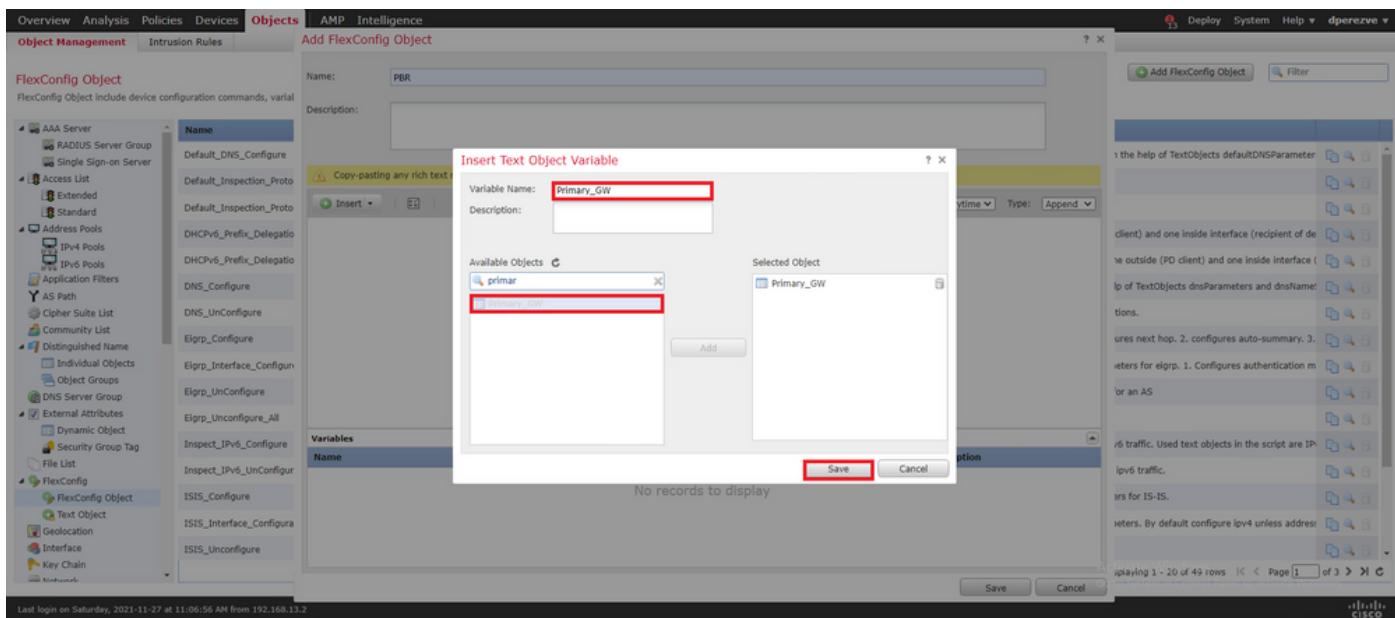


Además de la variable de route map, debemos agregar los objetos de texto FlexConfig que representan cada gateway (definidos en el paso 3). En el **Add FlexConfig Object** ventana diríjase a **Insert > Insert Policy Object > Text Object** .

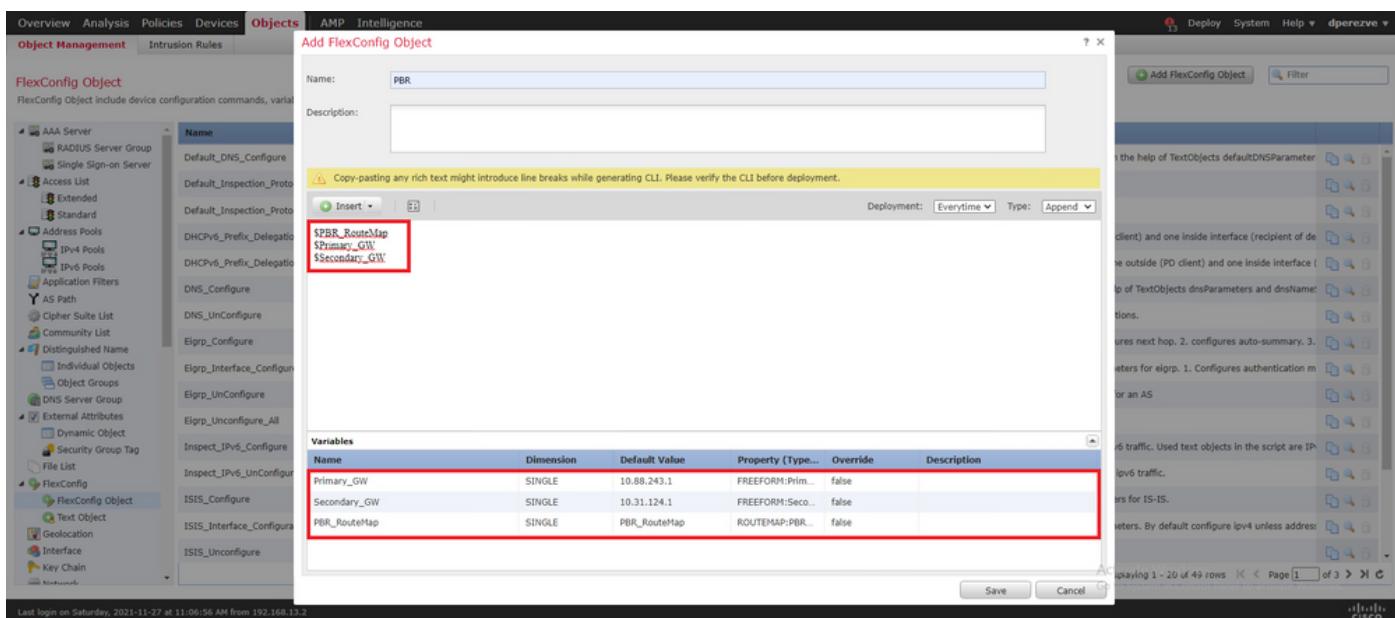


En el **Insert Text Object Variable** asigne un nombre a la variable y seleccione el objeto de texto que representa la puerta de enlace principal definida en el paso 3.

Haga clic en **Save** para agregarlo al objeto FlexConfig.



Repita estos últimos pasos para la puerta de enlace de copia de seguridad. Al final del proceso, las dos variables se deben anexar al objeto FlexConfig.

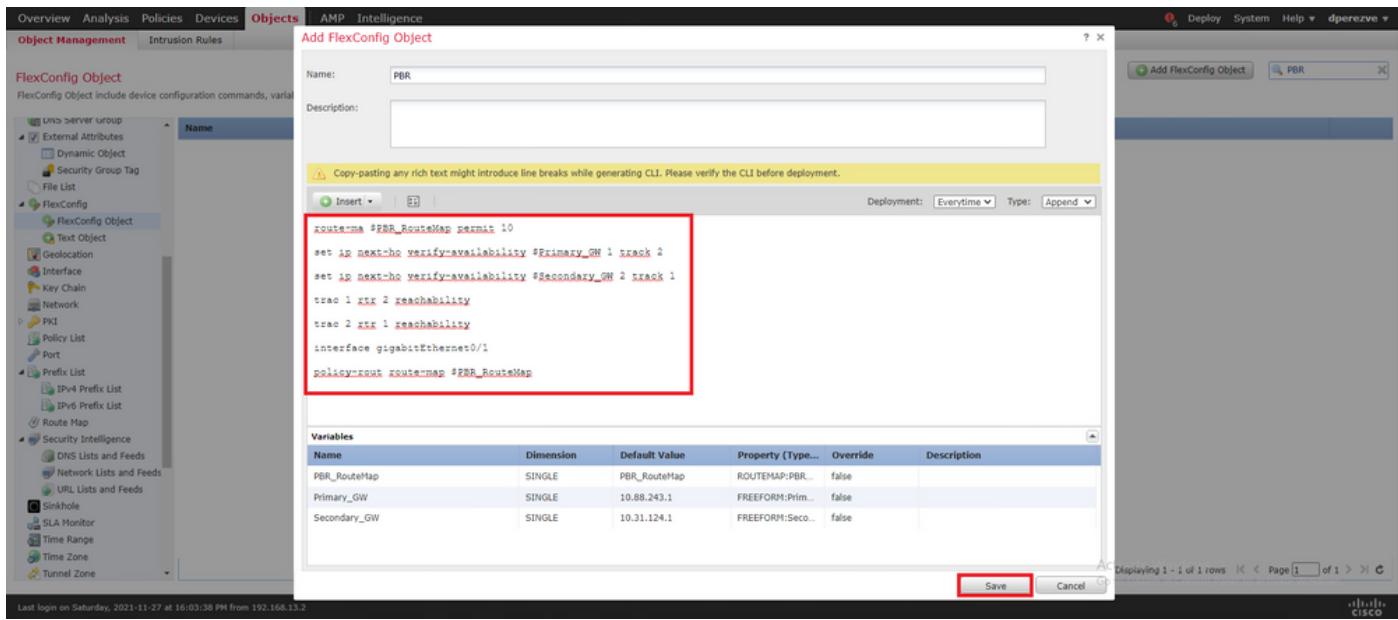


La sintaxis para la configuración PBR debe ser la misma que en Cisco ASA. El número de secuencia para el route map debe coincidir con el configurado en el Paso 2 (10 en este caso) así como con los ID de SLA.

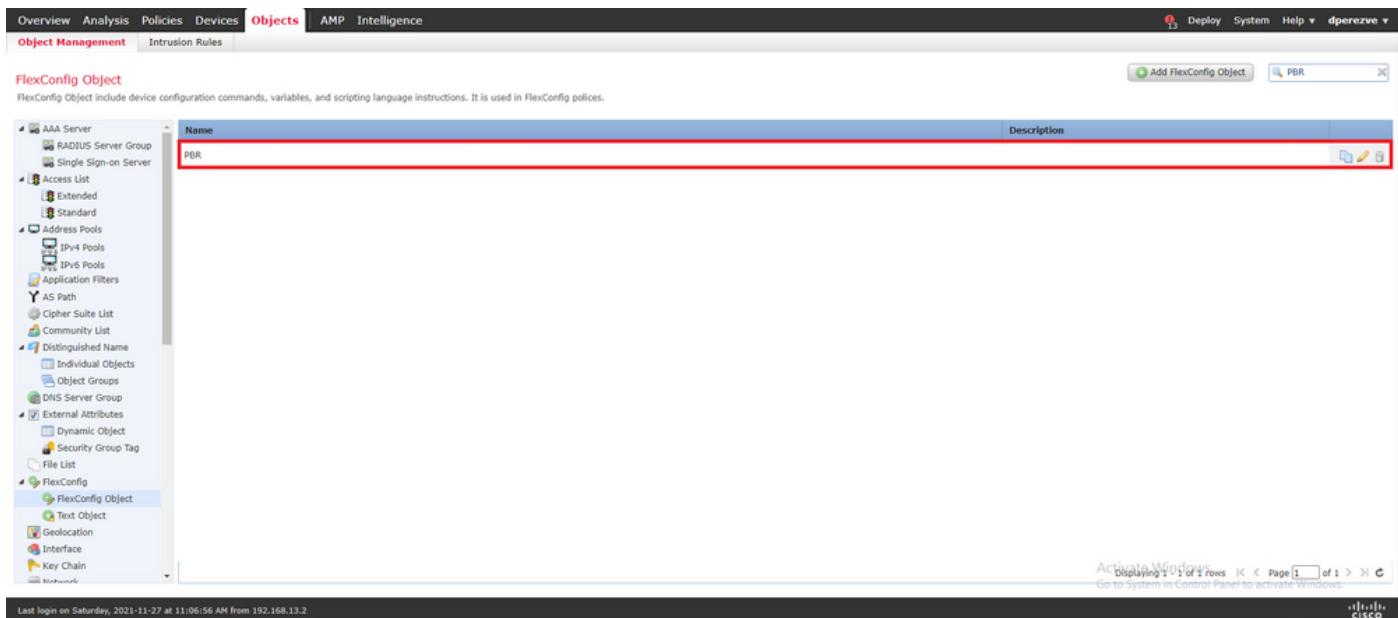
Para configurar PBR para comprobar la disponibilidad para el salto siguiente, el comando `set ip next-hop verify-availability` se debe utilizar el comando .

El mapa de ruta se debe aplicar a la interfaz interna, en este caso VLAN2813. Uso `policy-route route-map` bajo la configuración de la interfaz.

Haga clic en `Save` cuando se complete la configuración.



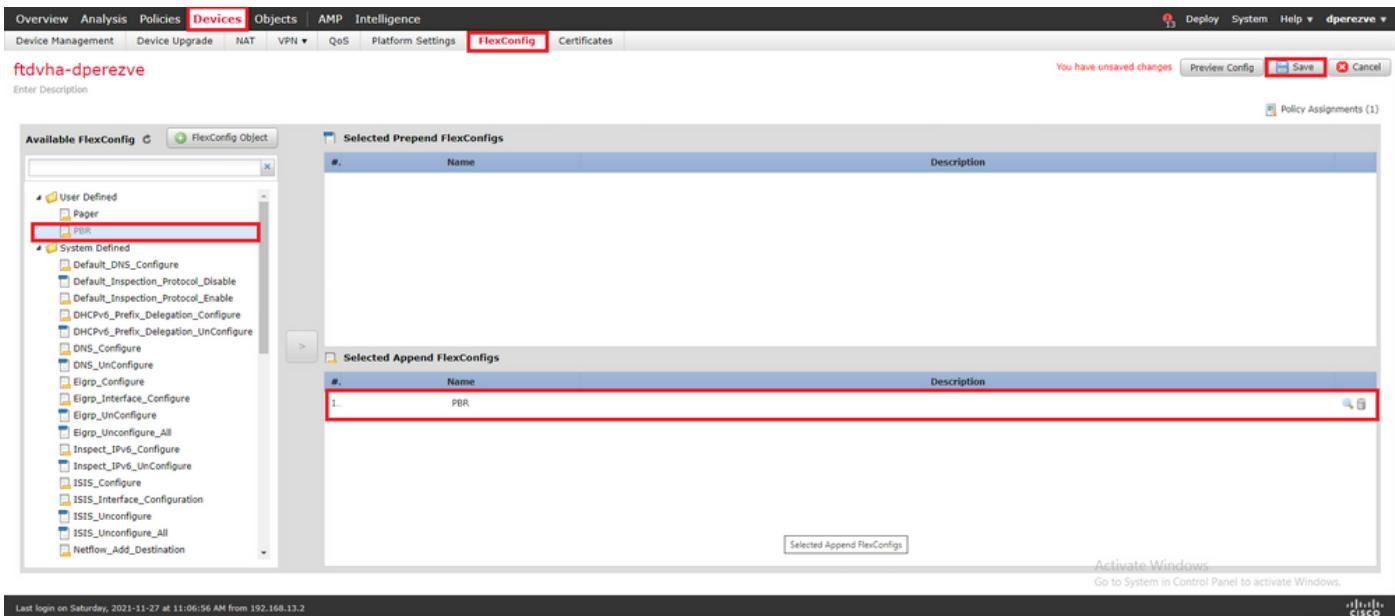
El objeto FlexConfig debe agregarse a la lista.



Paso 6. Asignación de un objeto FlexConfig PBR a una política FlexConfig

Desplácese hasta Devices > FlexConfig y editar la política FlexConfig disponible.

Seleccione el objeto FlexConfig de PBR en Available FlexConfig tabla de contenido, guardar cambios e implementar cambios en FTD.



Verificación

Una vez finalizada la implementación, el FTD debe enviar una solicitud de eco ICMP regular a los dispositivos supervisados para garantizar la disponibilidad. Mientras tanto, se debe agregar una ruta de la que se realiza un seguimiento al gateway principal a la tabla de routing.

```
firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address (access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2 [up] ip next-hop verify-availability 10.31.124.1 2 track 1 [up] firepower# show route Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static InterVRF Gateway of last resort is 10.88.243.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [1/0] via 10.88.243.1, VLAN230 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25 255.255.255.255 is directly connected, VLAN232 C 10.88.243.0 255.255.255.0 is directly connected, VLAN230 L 10.88.243.60 255.255.255.255 is directly connected, VLAN230 C 192.168.13.0 255.255.255.0 is directly connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813
```

Debido a que la conectividad con la puerta de enlace principal está activa, el tráfico de la subred interna (VLAN2813) debe reenviarse a través del circuito ISP principal.

```
firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed Phase: 1 Type: PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop verify-availability 10.31.124.1 2 track 1 Additional Information: Matched route-map PBR_RouteMap, sequence 10, permit Found next-hop 10.88.243.1 using egress ifc VLAN230 Phase: 2 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection
```

advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=176701, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN230(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170013860, priority=6, domain=nat, deny=false hits=168893, user_data=0x1461af306540, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN230(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,

port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188129, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176710, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172250,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=176702, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN230) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170013860, priority=6, domain=nat, deny=false hits=168894, user_data=0x1461af306540,

```

cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN230(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188130, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=176711, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any Error: not enough
buffer space to print ASP rule Result: input-interface: VLAN2813(vrfid:0) input-status: up
input-line-status: up output-interface: VLAN230(vrfid:0) output-status: up output-line-status:
up Action: allow

```

Si el FTD no recibe una respuesta de eco del gateway principal dentro del temporizador de umbral especificado en el objeto Monitor SLA, el host se considera inalcanzable y se marca como inactivo. La ruta de seguimiento al gateway principal también se reemplaza por la ruta de seguimiento al par de respaldo.

```

firepower# show route-map route-map PBR_RouteMap, permit, sequence 10 Match clauses: ip address
(access-lists): PBR_ACL Set clauses: ip next-hop verify-availability 10.88.243.1 1 track 2
[down] ip next-hop verify-availability 10.31.124.1 2 track 1 [up] firepower# show route Codes: L
- local, C - connected, S - static, R - RIP, M - mobile, B - BGP D - EIGRP, EX - EIGRP external,
O - OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2 E1
- OSPF external type 1, E2 - OSPF external type 2, V - VPN i - IS-IS, su - IS-IS summary, L1 -
IS-IS level-1, L2 - IS-IS level-2 ia - IS-IS inter area, * - candidate default, U - per-user
static route o - ODR, P - periodic downloaded static route, + - replicated route SI - Static
InterVRF Gateway of last resort is 10.31.124.1 to network 0.0.0.0 S* 0.0.0.0 0.0.0.0 [2/0] via
10.31.124.1, VLAN232 C 10.31.124.0 255.255.255.0 is directly connected, VLAN232 L 10.31.124.25
255.255.255.255 is directly connected, VLAN232 C 192.168.13.0 255.255.255.0 is directly
connected, VLAN2813 L 192.168.13.1 255.255.255.255 is directly connected, VLAN2813

```

El mensaje informativo 622001 se genera cada vez que el FTD agrega o quita una ruta de la tabla de ruteo.

```

firepower# show logg | i 622001 %FTD-6-622001: Removing tracked route 0.0.0.0 0.0.0.0
10.31.124.1, distance 2, table default, on interface VLAN232%FTD-6-305012: Teardown dynamic UDP
translation from VLAN2813:192.168.13.5/49641 to VLAN230:10.88.243.60/49641 duration 0:02:10

```

Ahora, todo el tráfico de VLAN2813 debe reenviarse a través del circuito ISP de respaldo.

```

firepower# packet-tracer input vlan2813 icmp 192.168.13.2 8 0 8.8.8.8 detailed Phase: 1 Type:
PBR-LOOKUP Subtype: policy-route Result: ALLOW Config: route-map PBR_RouteMap permit 10 match ip
address PBR_ACL set ip next-hop verify-availability 10.88.243.1 1 track 2 set ip next-hop
verify-availability 10.31.124.1 2 track 1 Additional Information: Matched route-map
PBR_RouteMap, sequence 10, permit Found next-hop 10.31.124.1 using egress ifc VLAN232 Phase: 2
Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list
CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-
end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-
list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information:
Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust
hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 3 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177180, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,

```

port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 4
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 5 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 6
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 7 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 8 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-
map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 9
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8251, user_data=0x1461af306740,
cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0),
output_ifc=VLAN232(vrfid:0) Phase: 10 Type: NAT Subtype: per-session Result: ALLOW Config:
Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,
domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 11
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 12 Type: ACCESS-LIST Subtype: log
Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip
ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_
remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-
id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields
rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729,
user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src
ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst
ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none
input_ifc=any, output_ifc=any Phase: 13 Type: CONN-SETTINGS Subtype: Result: ALLOW Config:
class-map class-default match any policy-map global_policy class class-default set connection
advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information:
Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set,
deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0,
protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0,
port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 14
Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic
VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in
id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740,

cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 15 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188612, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 16 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 17 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 18 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 19 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 20 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0, domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 21 Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true hits=177189, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 22 Type: ACCESS-LIST Subtype: log Result: ALLOW Config: access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced trust ip ifc VLAN2813 object VLAN2813 any rule-id 268437505 event-log flow-end access-list CSM_FW_ACL_ remark rule-id 268437505: PREFILTER POLICY: ftdvha-dperezve access-list CSM_FW_ACL_ remark rule-id 268437505: RULE: Internet_Traffic Additional Information: Forward Flow based lookup yields rule: in id=0x1461708f7a90, priority=12, domain=permit, trust hits=172729, user_data=0x146183cf8380, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any, ifc=VLAN2813(vrfid:0) dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 23 Type: CONN-SETTINGS Subtype: Result: ALLOW Config: class-map class-default match any policy-map global_policy class class-default set connection advanced-options UM_STATIC_TCP_MAP service-policy global_policy global Additional Information: Forward Flow based lookup yields rule: in id=0x146170d472a0, priority=7, domain=conn-set, deny=false hits=177181, user_data=0x146170d413f0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Phase: 24 Type: NAT Subtype: Result: ALLOW Config: nat (VLAN2813,VLAN232) after-auto source dynamic VLAN2813 interface Additional Information: Forward Flow based lookup yields rule: in id=0x146170032540, priority=6, domain=nat, deny=false hits=8252, user_data=0x1461af306740, cs_id=0x0, flags=0x0, protocol=0 src ip/id=192.168.13.0, mask=255.255.255.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=VLAN232(vrfid:0) Phase: 25 Type: NAT Subtype: per-session Result: ALLOW Config: Additional Information: Forward Flow based lookup yields rule: in id=0x1461af9c3320, priority=0,

```
domain=nat-per-session, deny=true hits=188613, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=0 src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any, dscp=0x0, nsg_id=none input_ifc=any, output_ifc=any Phase: 26
Type: IP-OPTIONS Subtype: Result: ALLOW Config: Additional Information: Forward Flow based
lookup yields rule: in id=0x1461aff02da0, priority=0, domain=inspect-ip-options, deny=true
hits=177190, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0 src ip/id=0.0.0.0,
mask=0.0.0.0, port=0, tag=any dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0,
nsg_id=none input_ifc=VLAN2813(vrfid:0), output_ifc=any Result: input-interface:
VLAN2813(vrfid:0) input-status: up input-line-status: up output-interface: VLAN232(vrfid:0)
output-status: up output-line-status: up Action: allow
```

Troubleshoot

Para validar qué entrada PBR se exige en interesting traffic ejecute el comando **debug policy-route**.

```
firepower# debug policy-route debug policy-route enabled at level 1 firepower# pbr: policy based
route lookup called for 192.168.13.5/45951 to 208.67.220.220/53 proto 17 sub_proto 0 received on
interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule from ACL(2) pbr: route map
PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr: evaluating verified next-hop
10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230 : next_hop = 10.88.243.1
pbr: policy based route lookup called for 192.168.13.5/56099 to 208.67.220.220/53 proto 17
sub_proto 0 received on interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule from
ACL(2) pbr: route map PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr:
evaluating verified next-hop 10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230
: next_hop = 10.88.243.1 pbr: policy based route lookup called for 192.168.13.2/24 to 8.8.8.8/0
proto 1 sub_proto 8 received on interface VLAN2813, NSGs, nsg_id=none pbr: First matching rule
from ACL(2) pbr: route map PBR_RouteMap, sequence 10, permit; proceed with policy routing pbr:
evaluating verified next-hop 10.88.243.1 pbr: policy based routing applied; egress_ifc = VLAN230
: next_hop = 10.88.243.1 pbr: policy based route lookup called for 192.168.13.5/40669 to
208.67.220.220/53 proto 17 sub_proto 0 received on interface VLAN2813, NSGs, nsg_id=none
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).